

11/80/1998
USPTO
11/08/98IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
UTILITY PATENT APPLICATION TRANSMITTAL
UNDER 37 CFR 1.53(b)

Address to:	Attorney Docket No.	TU999050
Assistant Commissioner for Patents	Inventor(s)	PAUL JOSEPH SEGER
Box Patent Application	Express Mail Label No.	10678 U 435899 11/08/98
Washington, DC 20231	Total Pages	53

Title of Application:
WIRELESS SECURITY ACCESS MANAGEMENT FOR A PORTABLE DATA STORAGE CARTRIDGE

Transmitted with the patent application are the following:

43 Page(s) Specification, claims, abstract
4 Page(s) Informal drawing sheets
2 Page(s) Declaration and Power of Attorney
1 Page(s) Recordation of Assignment
1 Page(s) Assignment of the Invention to International Business Machines Corporation
2 Page(s) Information Disclosure Statement (IDS)
(citation copies not included in number of pages)
0 Page(s) Preliminary Amendment

This application is a: Continuation Divisional Continuation-in-Part of prior application Serial No. _____
filed on _____.

Fee Calculation

	Claims Filed		Extra	Rate	Fees
Basic Fee					\$760.00
Total Claims	50	-20	30	x\$18.00	\$540.00
Independent Claims	4	-3	1	x\$78.00	\$78.00
Multiple Dependent Claim				260.00	
				TOTAL	\$1,378.00

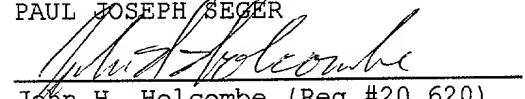
Please charge my Deposit Account No. 09-0449 in the amount of
\$1378.00. A duplicate copy of this sheet is attached.

The Commissioner is hereby authorized to charge payment of the
following fees associated with this communication or credit any
overpayment to Deposit Account 09-0449. A duplicate copy of this sheet
is attached.

Any filing fees under 37 CFR 1.16 for the presentation of extra
claims.

Any patent application processing fees under 37 CFR 1.17.

Respectfully submitted,
PAUL JOSEPH SEGER


John H. Holcombe (Reg. #20,620)
Attorney for Applicant
Telephone: 520-760-6629
From: IBM Corporation
Intellectual Property Law
9000 S. Rita Road (90A/9032)
Tucson, Arizona 85744

**WIRELESS SECURITY ACCESS MANAGEMENT
FOR A PORTABLE DATA STORAGE CARTRIDGE**

FIELD OF THE INVENTION

This invention relates to the protection of data stored in 5 portable data storage cartridges, and, more particularly, to providing secure access to the data stored in portable data storage cartridges.

BACKGROUND OF THE INVENTION

Data storage cartridges are typically employed to store data 10 which may be transported between data storage drives and may be stored separately from the data storage drives between uses. Much of the data must be secured with respect to outsiders, and much of the data must be secured in favor of some users with respect to other users. Only certain users should be allowed 15 access to certain data, and certain users should be allowed to define who has access to that data. An example comprises payroll information, and another example comprises financial account information. Further, the authorized users tend to change over time.

Thus, it is advantageous to not only provide security for data stored in data storage cartridges, but also to manage the access to that data to particular users, and to different users for different data storage cartridges.

5 Security of data stored in portable data storage cartridges is typically managed by encrypting the data and providing a key for decrypting the data. Typically, a data processing system includes or obtains the decryption key, and users which are authorized access to the data are listed in the data processing 10 system. The data processing system provides the key and decrypts the data of the data storage drive accessing the data storage cartridge. One example is described in U.S. Patent No. 5,857,021 in which permission data is written into the data storage media of the cartridge which contains an encrypted key that is 15 necessary for decrypting the data. The key can be decoded only with valid IDs of the equipment of the data processing system. The data processing system thus provides the decrypting key and the user is authorized access by a table in the data processing system.

20 A difficulty is that the access by a user to the data is not portable even though the data storage cartridge is portable. The access by a user is limited to a data processing system having the authorization table and having the decryption key.

Data processing systems are continually being updated and the authorization tables must be transferred to the new system, and correlated with the data storage media to which access is required. The management of the authorization table is typically 5 handled by other organizations, such as IS, than those responsible for the security of the data. The changes to the table and correlation to the data and to the various data processing systems become a source of loss of security.

SUMMARY OF THE INVENTION

10 An object of the present invention is to provide a security system which is portable and may be managed to accommodate changes to access to the data.

Disclosed is a portable security system, method, and computer readable program code of a computer program product, 15 which resides in a portable data storage cartridge for managing access to the portable data storage cartridge. The data storage cartridge has a data storage media, such as a magnetic tape or an optical disk, for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive.

20 The portable security system comprises a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive

DOCKET: TU999050

when mounted in the data storage drive. The wireless interface preferably comprises an RF interface. A programmable computer processor is mounted in the portable data storage cartridge and coupled to the wireless interface. The computer processor within 5 the portable data storage cartridge is powered by the wireless interface and receives and transmits data to the data storage drive via the wireless interface. The computer processor provides a user table comprising at least one unique user identifier for each authorized user, which may comprise a user 10 symbol and a corresponding user key, and at least one permitted activity the user is authorized to conduct with respect to the data storage media. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user. 15 The computer processor within the portable data storage cartridge receives user authentication messages from the data storage drive via the wireless interface, and combines the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny 20 the user activity, and transmits the user authorization or denial to the data storage drive via the wireless interface.

Preferably, a private key, public key cryptographic algorithm is employed. Thus, each user identifier in the user table comprises a user symbol and the user's decrypting sender

DOCKET: TU999050

public key, wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, specifically comprising a request for access encrypted by a sender private key and a receiver public key, and wherein the employed private key, public key cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key, whereby the user authentication message is known to have come from the user.

10 The permitted activities in the user table may comprise 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read the user entry of the user table, 4) read all entries of the user table, 5) add entries to the user table, and 6) change/delete entries to 15 the user table. Each of the users may be authorized to conduct selected ones of the plurality of activities.

A class table is additionally provided that has an unique class identifier for each authorized class of users, which may comprise a class symbol and a corresponding class key and at 20 least one permitted activity each class of users is authorized to conduct with respect to the data storage media. The class identifier, when combined with a user authentication message from a user of the authorized class of users in accordance with the predetermined algorithm, authorizes the user. The user table

DOCKET: TU999050

additionally comprises any class membership of each user, wherein the user may be authorized with respect to the class table either by the class authorization or by the user authorization. The user table permitted activities may additionally comprise 3) read 5 all entries of the class table, 4) add entries to the class table, and 5) change/delete entries to the class table.

For a fuller understanding of the present invention, reference should be made to the following detailed description taken in conjunction with the accompanying drawings.

10

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagrammatic representation of a data storage cartridge with a data storage drive and a host in accordance with the present invention;

15 FIG. 2 is a block diagram of an RF interface, computer processor, and nonvolatile storage in the data storage cartridge of FIG. 1;

FIGS. 3 and 4 are diagrammatic representations of tables of the nonvolatile storage of FIG. 2;

20 FIG. 5 is a diagrammatic representation of the encryption of a request for access and its decryption in accordance with the present invention;

FIG. 6 is a diagrammatic representation of a state diagram of the operation of the computer processor of FIG. 2 in accordance with the present invention; and

FIGS. 7 and 8 are flow charts depicting the method of the 5 present invention for initializing a data storage cartridge and for conducting the authentication and authorization of a user request.

DETAILED DESCRIPTION OF THE INVENTION

This invention is described in preferred embodiments in the 10 following description with reference to the Figures, in which like numbers represent the same or similar elements. While this invention is described in terms of the best mode for achieving 15 this invention's objectives, it will be appreciated by those skilled in the art that variations may be accomplished in view of these teachings without deviating from the spirit or scope of the invention.

Referring to FIG. 1, a data storage cartridge 10, such as a magnetic tape cartridge (as illustrated) or an optical disk, is loaded into a data storage drive 11. An example of a data 20 storage cartridge is an IBM 3590 data tape cartridge. Another example is an LTO (Linear Tape Open) data tape cartridge.

The data storage cartridge has a storage media **12**, such as a magnetic tape, that is stored on a tape reel **15** and may be threaded into the data storage drive **11**. As an example, the magnetic tape **12** is threaded past a read/write head **17** to a **5** take-up reel **18**. A drive controller **20**, which includes both read/write electronics and control circuitry for operating the drive, is coupled to the read/write head **17** for reading data from, or writing data to, the storage media **12**. The drive controller is also coupled, via an interface **21**, to a host **22**. **10** The host may comprise a data processing system or server, or may comprise a drive subsystem controller, for example, for an automated data storage library. An example of a data storage drive is an IBM 3590 tape storage subsystem.

The data storage drive **11** is modified so that drive **15** controller **20** is also coupled to a wireless interface **25**. The data storage cartridge **10** is also modified to incorporate a wireless interface **26** and a computer processor **30** with a nonvolatile memory **31**.

The cartridge wireless interface **26** receives power and data **20** from, and sends data to, the wireless interface **25** of the data storage drive when the data storage cartridge **10** is mounted in the data storage drive **11**. Preferably, the wireless interface **25, 26** is an RF wireless interface. An example is described in

U.S. Patent No. 4,941,201. A high frequency inductive wireless interface may also be employed, which is of sufficiently high frequency that the magnetic storage media **12** is not adversely affected by the signal. Examples are described in U.S. Patents 5 No. 4,650,981, No. 4,758,836, and No. 3,859,624. Alternatively, the inductive antennae for the wireless interface are shielded from the magnetic storage media **12**.

The computer processor **30** comprises a microprocessor chip, for example, an Intel Pentium chip arranged to operate in a low 10 power environment, such as a portable computer, and the associated nonvolatile memory **31** is also arranged to operate in a low power environment.

In accordance with the present invention, the wireless interface **26** and the computer processor **30** with the associated 15 nonvolatile memory **31** are mounted in, and provide a portable security system for, the portable data storage cartridge **10**. Specifically, the security system, by being mounted in the portable data storage cartridge, becomes portable, accompanying the cartridge at all times. Thus, the security is no longer 20 exclusively dependent upon the security of the data storage drive **11** and its host system **22**, and is not limited to a particular drive or host. The cartridge may be used with different drives and host systems at varied locations, and may be used with

DOCKET: TU999050

updated drives and updated data processing systems. Further, the security system may be managed and updated to change access to the data at any of the drives by users which have previously been granted permission via the user or class tables in the data 5 storage cartridge. The security system remains portable and within the data storage cartridge.

The wireless interface 26 and computer processor 30 are detailed in FIG. 2. An antenna 35 receives the RF signal from the RF interface of the data storage drive, and coupler 36 10 supplies the received signal to a power conversion circuit 40, and to a data demodulator 42. The power conversion circuit 40 converts the received signal to a power current, supplying the current on line 44 to all of the devices in the data storage cartridge requiring power, including the computer processor 30, 15 the data demodulator 42, and a data modulator 45. The received signal from antenna 35 is encoded, and data demodulator 42 receives the incoming coded signal from coupler 36 and demodulates the signal to provide data signals to the computer processor 30. Data signals from the computer processor 30 are 20 provided to the data modulator 45 which encodes the signals for transmission by coupler 36 and antenna 35 to the RF interface of the data storage drive.

The computer processor **30** is a programmable computer processor comprising a microprocessor **37** having computer readable program code embodied therein, including an encryption/decryption algorithm **38** and an authorization/authentication/permited activities algorithm **39**. The nonvolatile storage **31** is employed to store user and class tables, as will be explained. The nonvolatile storage may comprise a separate chip attached to the programmable computer processor **30** and its microprocessor **37**, or may comprise a portion of the same chip. The computer readable program code may be stored in a nonvolatile internal memory of the computer processor **30** or may also be stored in the nonvolatile memory **31**, and loaded into the computer processor **30**. The algorithms **38** and **39** may be preloaded into the programmable computer processor **30**, or may be supplied to the computer processor at initialization over the wireless interface **26**.

The computer processor **30**, employing the algorithm **39**, provides a user table in nonvolatile memory **31** comprising at least a unique user identifier for each authorized user, which may comprise a user symbol and a corresponding key, and at least one permitted activity the user is authorized to conduct with respect to the data storage media, and provides a class table in nonvolatile memory **31** which has unique class identifier for each authorized class of users, which may comprise a class symbol and

a corresponding key, and at least one permitted activity each class of users is authorized to conduct with respect to the data storage media.

In accordance with the predetermined algorithm **39**, the user identifier, when combined with a user authentication message from the authorized user, employing the encryption/decryption algorithm **38**, authorizes the user. The computer processor **30** receives user authentication messages from the data storage drive via the wireless interface **26**, and combines the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm **39** and encryption/decryption algorithm **38** to authorize or deny the user activity, and transmits the user authorization or denial to the data storage drive via the wireless interface **26**.

15 Herein, the encryption/decryption algorithm **38** comprises any suitable encryption/decryption algorithm which both provides security and portability. Examples of algorithms which provide security and portability are the "public key" cryptography algorithms. U.S. Patent No. 4,405,829 describes a "public key" 20 encryption/decryption algorithm that has become a defacto-standard, often called the "RSA" cryptosystem after the names of the authors. An implementation that provides authentication and allows authorization as employed herein is described in U.S. Patent No. 4,748,668. Accordingly, the user

identifier comprises a user symbol and a user decrypting sender public key. When combined with a user authentication message from the authorized user that is encrypted by a receiver public key, the user is authorized. Additionally, with the use of a 5 sender private key and the receiver public key, the authentication message can be encrypted so that, with the use of a receiver private key and the sender public key, the authentication message is both decrypted and the message is known to have come from the sender.

10 FIGS. 3, 4 and 5 illustrate examples of cartridge initialization with the user and class tables and the operation of the algorithm 39 employing the cryptography algorithm 38.

FIG. 3 illustrates an uninitialized data storage cartridge 10 either without user and class tables, or which has established 15 user and class tables, but which are empty. FIG. 4 illustrates the data storage cartridge 10 after the user table 50 and the class table 51 have been initialized in accordance with the present invention.

As discussed above, the computer processor 30 provides the 20 user table 50 with at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media. Preferably, each user identifier in the user table 50 comprises a

user symbol **54** and a user decrypting sender public key **55**. The permitted activities **56** of the user may comprise a separate entry for each user identifier and permitted activity that the user is authorized to conduct. Alternatively, the user table may 5 comprise a separate entry for each user identifier, the entry comprising all of the permitted activities that the user is authorized to conduct. The user table **50** additionally comprises any class membership **57** of each user, so that the user may be authorized with respect to the class table **51** by the user 10 authorization.

In accordance with the present invention, the class table **51** is provided that has an unique class identifier for each authorized class of users, and at least one permitted activity **64** that each class of users is authorized to conduct. Preferably 15 each class identifier in the class table **51** comprises a class symbol **62** and a class decrypting sender public key **63**. The class identifier, when combined with a user authentication message from a user of the authorized class of users in accordance with the predetermined algorithm, authorizes the user. Thus, the user may 20 be authorized with respect to the class table either by the class authorization or by the user authorization **57**.

The permitted activities **64** of the members of the class may comprise a separate entry for each class identifier and permitted

activity that the user/class member is authorized to conduct. Alternatively, the class table may comprise a separate entry for each class identifier, the entry comprising all of the permitted activities that the user/class member is authorized to conduct.

5 The permitted activities **56** in the user table **50** may comprise 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read user entry of the user table, 4) read all entries of the user table, 5) add entries to the user table, 6) change/delete entries 10 to the user table, 7) read class entry of the class table, 8) read all entries of the class table, 9) add entries to the class table, 10) change/delete entries to the class table, and 11) change the receiver private key.

The permitted activities **64** in the class table **51** may comprise 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read the user's class entry of the class table, 4) read all entries of the class table, 5) add entry to the class table, 6) change/delete entries to the class table, 7) read all entries of 20 the user table, 8) add entries to the user table, 9) change/delete entries to the user table and 10) change the receiver private key.

The operation of a public key algorithm for authorizing access is illustrated with respect to FIG. 5. The preferred

implementation is one as described above which both allows an authentication message to be decrypted, and also provides a "signature" assuring that the authentication message has come from the sender. In one example, the user/class symbol will have 5 been sent. A user/class member generates an authentication message 70. Preferably, the authentication message includes the request for access to conduct the desired activity, saving a need for a second message. The user/class member has a sender private key 71 which is employed, together with a receiver public key 72, 10 to encrypt the authentication message. The receiver public key 72 is made known to the users and class members and is mathematically related to the sender private key, as discussed in the '668 patent, but the message cannot be decrypted with the same keys. The message instead is only readable by the intended 15 receiver because of the use of the receiver public key. When decrypted, the message must have therefore been intended for the receiver. Thus, at the cartridge, the algorithm of the computer processor decrypts the message employing a receiver private key 73 and a sender public key 74. As discussed above, the sender 20 public key has been made available and is kept in the user table or in the class table. Thus, if the keys decrypt the encrypted authentication message, the message is known to have come from the sender who is the user/class member. This is known as providing an authentication "signature".

As the result, the user/class member may rely on the security of the portable security system, method, and computer readable program code of a computer program product, of the present invention, which resides in a portable data storage 5 cartridge for managing access to the portable data storage cartridge.

A state diagram of the operation of the computer processor in accordance with the present invention is illustrated in FIG. 6, and flow charts of the method of the present invention are 10 depicted in FIGS. 7 and 8.

Referring to FIGS. 1 and 7, the initialization of an uninitialized cartridge 10 is initiated at step 80. The cartridge is loaded into a drive 11 having a wireless interface 25, and, in step 81, the initialization information is 15 transmitted to the cartridge. The initialization information is not encrypted, and is provided when in a secure situation. The cartridge wireless interface 26 receives the initialization information in step 82 and provides the information to the cartridge processor 30. As discussed above, the initialization 20 information comprises the user and class tables. The cartridge processor 30, in step 83, recognizes that the input from the wireless interface is initialization information, and determines whether the cartridge is uninitialized. If the cartridge has

DOCKET: TU999050

been initialized previously, a message is sent to the drive **11** over the wireless interface, in step **84**, denying the initialization.

If the cartridge is uninitialized, an initializing drive or **5** host computer provides the user table to the cartridge computer processor **30** in step **85** and provides the class table in step **86**, both via the wireless interface. The receiver private key may have been provided previously, or, as an optional step **87**, may be provided in the initialization load. The initialization is then **10** complete, and the drive is informed of the completion in step **89**.

Referring to FIGS. **1**, **6** and **8**, an authentication or an access request is initiated in step **90**, e.g., by sending the user symbol, and the cartridge computer processor **30** is initially in an idle state **91**. In step **93**, the request is received at the **15** wireless interface **26** and is provided to the computer processor. The computer processor moves to state **94** and, in step **95**, determines whether the requesting user or class member is in the list of the user or class table. If not in the table, the computer processor **30**, in step **96**, moves to state **97** and denies **20** access to the user/class member via the wireless interface **26**.

If the user or class member is in the respective table, the computer processor, in step **98**, moves to state **99** and requests the authentication message from the user or class member. The

computer processor moves to state 100 while awaiting the authentication message, and, if the message is not received in a time out period, denies access in state 97. In step 102, the authentication message is received by the wireless interface 26 5 and forwarded to the computer processor 30. As discussed above, the authentication message is encrypted by the sender private key and the receiver (cartridge) public key. The computer processor moves to state 103, receiving the message and beginning the authentication. In step 105, the computer processor conducts the 10 decryption of the authentication message employing the receiver private key and employing the sender public key from the user or class table. In step 106, the computer processor determines whether the user or class member is authorized. If not, the computer processor 30 moves to state 97 and, in step 96, denies 15 access.

If the user or class member is authorized, the computer processor moves to state 98 and, in step 110, reads the user or class table for the permitted activities for the user/class member. As discussed above, the authentication message 20 preferably includes a request to conduct one or more activities. Based on the permitted activities of the user or class table and the request, the computer processor moves to state 111 or to state 112 to grant the permitted activity. The permission to

change the receiver private key will be very limited to a particular user or to a particular class. Thus, the grant of the permitted activities of state **111** are transmitted in step **114** to the drive **11** over the wireless interface. As an example, the **5** requested access from state **111** does not require a decrypting key for the data, such as changing an entry to the user table. State **112** is entered only in response to a specific request by the user/class member, and, in step **114**, the decrypting key for the data on the cartridge data storage media is transmitted to the **10** drive **11** from the cartridge **10** over the wireless interface **26**. The computer processor then moves back to the idle state **91**, and the data may be read.

As specific security examples, read access to the data stored in the data storage media is controlled by the computer **15** processor **30** in the portable cartridge through the decrypting key; table access is enforced by the computer processor **30** in the portable cartridge; and write access is controlled logically in the drive, which may be under the logical control of the processor. However, the cartridge itself cannot totally restrict **20** writing per se.

Thus, the present invention provides a security system which is portable and may be managed to accommodate changes to access to the data of the data storage cartridge **10**. Only certain users

DOCKET: TU999050

are allowed access to each cartridge, and only certain users are allowed to define who has access to that data.

While the preferred embodiments of the present invention have been illustrated in detail, it should be apparent that 5 modifications and adaptations to those embodiments may occur to one skilled in the art without departing from the scope of the present invention as set forth in the following claims.

I claim:

DOCKET: TU999050

1 A portable security system for managing access to a portable data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive,

5 said portable security system comprising:

 a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive; and

10 a computer processor mounted in said portable data storage cartridge and coupled to said wireless interface; said computer processor powered by said wireless interface and receiving and transmitting data to said data storage drive via said wireless interface; said computer processor having a user table comprising
15 at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm,
20 authorizes said user; said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user

DOCKET: TU999050

activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface.

2. The portable security system of **Claim 1**, wherein said wireless interface comprises an RF interface.

5 3. The portable security system of **Claim 1**, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said computer processor 10 conducts said combination by decrypting said user authentication message by said user decrypting key.

4. The portable security system of **Claim 3**, wherein said user decrypting key comprises a sender public key, and wherein said predetermined algorithm comprises a public key cryptographic 15 algorithm.

5. The portable security system of **Claim 4**, wherein said user authentication message is encrypted by a sender private key and a receiver public key, and wherein said public key cryptographic algorithm decrypts said user authentication message employing a

DOCKET: TU999050

receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

6. The portable security system of Claim 1, wherein said computer processor user table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table.

7. The portable security system of Claim 1, wherein said computer processor user table comprises a separate entry for each said user identifier and said permitted activity said user is authorized to conduct.

8. The portable security system of Claim 1, wherein said computer processor user table comprises a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct.

9. The portable security system of Claim 1, wherein said computer processor additionally comprises a nonvolatile memory storing said user table.

10. The portable security system of Claim 1, wherein said 5 computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to conduct with respect to said data storage media, said class identifier, when combined with a user 10 authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user; and wherein said computer processor additionally, upon receiving said user authentication messages from said data storage drive via said wireless interface, combining said user 15 authentication message with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user, and transmitting said class authorization or denial to said data storage drive via said wireless interface.

20 11. The portable security system of Claim 10, wherein said computer processor user table additionally comprises any class membership of each said user, wherein said user may be authorized

DOCKET: TU999050

with respect to said class table either by said class authorization or by said user authorization.

12. The portable security system of Claim 10, wherein said computer processor user table and said class table permitted 5 activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read all entries of said class 10 table, 4) add entries to said class table, and 5) change/delete entries to said class table.

13. The portable security system of Claim 10, wherein said computer processor additionally comprises a nonvolatile memory storing said user table and said class table.

15 14. The portable security system of Claim 1, wherein said data stored in said data storage media is encrypted, wherein said computer processor user table permitted activities comprise at least 1) read access to data stored in said data storage media, and wherein said user authorization for said read access 20 additionally comprises a decryption key for said encrypted stored data.

15. A data storage cartridge for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, comprising:

data storage media mounted in said data storage cartridge

5 for storing said data for said read/write access;

a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive; and

10 a computer processor mounted in said portable data storage cartridge and coupled to said wireless interface; said computer processor powered by said wireless interface and receiving and transmitting data to said data storage drive via said wireless interface; said computer processor having a user table comprising

15 at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm,

20 authorizes said user; said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user

DOCKET: TU999050

activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface.

16. The data storage cartridge of Claim **15**, wherein said wireless interface comprises an RF interface.

5 **17.** The data storage cartridge of Claim **15**, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said computer processor
10 conducts said combination by decrypting said user authentication message by said user decrypting key.

18. The data storage cartridge of Claim **17**, wherein said user decrypting key comprises a sender public key, and wherein said predetermined algorithm comprises a public key cryptographic
15 algorithm.

19. The data storage cartridge of Claim **18**, wherein said user authentication message is encrypted by a sender private key and a receiver public key, and wherein said public key cryptographic algorithm decrypts said user authentication message employing a

receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

20. The data storage cartridge of Claim 15, wherein said computer processor user table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table.

21. The data storage cartridge of Claim 15, wherein said computer processor user table comprises a separate entry for each said user identifier and said permitted activity said user is authorized to conduct.

22. The data storage cartridge of Claim 15 wherein said computer processor user table comprises a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct.

23. The data storage cartridge of Claim 15, wherein said computer processor additionally comprises a nonvolatile memory storing said user table.

24. The data storage cartridge of Claim 15, wherein said 5 computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to conduct with respect to said data storage media, said class identifier, when combined with a user 10 authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user; and wherein said computer processor additionally, upon receiving said user authentication messages from said data storage drive via said wireless interface, combining said user 15 authentication message with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user, and transmitting said class authorization or denial to said data storage drive via said wireless interface.

20 25. The data storage cartridge of Claim 24, wherein said computer processor user table additionally comprises any class membership of each said user, wherein said user may be authorized

with respect to said class table either by said class authorization or by said user authorization.

26. The data storage cartridge of Claim **24**, wherein said computer processor user table and said class table permitted 5 activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read all entries of said class 10 table, 4) add entries to said class table, and 5) change/delete entries to said class table.

27. The data storage cartridge of Claim **24**, wherein said computer processor additionally comprises a nonvolatile memory storing said user table and said class table.

15 **28.** The data storage cartridge of Claim **15**, wherein said data stored in said data storage media is encrypted, wherein said computer processor user table permitted activities comprise at least 1) read access to data stored in said data storage media, and wherein said user authorization for said read access 20 additionally comprises a decryption key for said encrypted stored data.

29. A method for providing a portable secure interface to a data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, and 5 a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive, said data storage cartridge having a user table comprising at least a unique user identifier for each authorized user and at 10 least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user, said method comprising the steps of: 15 receiving said user authentication messages from said data storage drive via said wireless interface; combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity; 20 and transmitting said user authorization or denial to said data storage drive via said wireless interface.

DOCKET: TU999050

30. The method of Claim 29, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user 5 decrypting key, and wherein said combining step comprises decrypting said user authentication message by said user decrypting key.

31. The method of Claim 30, wherein said user decrypting key comprises a sender public key, and wherein said predetermined 10 algorithm comprises a public key cryptographic algorithm.

32. The method of Claim 31, wherein said user authentication message is encrypted by a sender private key and a receiver public key, wherein said public key cryptographic algorithm decrypts said user authentication message employing a receiver 15 private key and said sender public key, and wherein said combining step comprises decrypting said user authentication message by said receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

20 33. The method of Claim 29, wherein said user table comprises a plurality of said permitted activities, selected ones of which

DOCKET: TU999050

each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read 5 all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table; and wherein said transmitting step comprises transmitting authorization to conduct the selected said user permitted activities said user is authorized to conduct.

10 34. The method of Claim 29, wherein said user table comprises a separate entry for each said user identifier and said permitted activity said user is authorized to conduct; and wherein said transmitting step additionally comprises identifying said user permitted activities from said separate entries.

15 35. The method of Claim 29, wherein said step of providing said user table comprises a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct; and wherein said transmitting step additionally comprises identifying said user permitted 20 activities from said user separate entry.

36. The method of Claim 29, wherein said data storage cartridge additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity said class of users is authorized to 5 conduct with respect to said data storage media, said class identifier, when combined with a user authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user;

wherein said combining step additionally comprises, upon

10 receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user; and

15 wherein said transmitting step additionally comprises transmitting said class authorization or denial to said data storage drive via said wireless interface.

37. The method of Claim 36, wherein said user table additionally comprises any class membership of each said user; and wherein 20 said combining step additionally authorizes said user with respect to said class table either by said class authorization or by said user authorization.

38. The method of Claim **36**, wherein said user table and said class table comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table; and wherein said transmitting step comprises transmitting authorization to conduct the selected said user and said class permitted activities said user is authorized to conduct.

39. The method of Claim **29**, wherein said data stored in said data storage media is encrypted, wherein said step of providing said user table permitted activities comprises providing at least 15 1) read access to data stored in said data storage media, and wherein said step of transmitting said user authorization for said read access additionally comprises transmitting a decryption key for said encrypted stored data.

40 A computer program product usable with a programmable computer processor having computer readable program code embodied therein for providing a secure interface to a data storage cartridge, said programmable computer processor mounted in said 5 data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, and a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, 10 said data storage drive when mounted in said data storage drive, said computer program product comprising:

computer readable program code which causes said programmable computer processor to provide a user table comprising at least a unique user identifier for each authorized 15 user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user;

20 computer readable program code which causes said programmable computer processor to receive said user authentication messages from said data storage drive via said wireless interface;

computer readable program code which causes said programmable computer processor to combine said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to

5 authorize or deny said user activity; and

computer readable program code which causes said programmable computer processor to transmit said user authorization or denial to said data storage drive via said wireless interface.

10 **41.** The computer program product of Claim 40, wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said computer readable
15 program code additionally causes said programmable computer processor to conduct said combination by decrypting said user authentication message by said user decrypting key.

42. The computer program product of Claim 41, wherein said user decrypting key comprises a sender public key, and wherein said
20 predetermined algorithm comprises a public key cryptographic algorithm.

43. The computer program product of Claim 42, wherein said user authentication message is encrypted by a sender private key and a receiver public key, wherein said public key cryptographic algorithm decrypts said user authentication message employing a receiver private key and said sender public key, and wherein said computer readable program code additionally causes said programmable computer processor, in conducting said combination, to decrypt said user authentication message by said receiver private key and said sender public key, whereby said user authentication message is known to have come from said user.

44. The computer program product of Claim 40, wherein said computer readable program code additionally causes said programmable computer processor to provide in said user table a plurality of said permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored in said data storage media, 3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table.

45. The computer program product of Claim 40, wherein said computer readable program code additionally causes said

programmable computer processor to provide in said user table a separate entry for each said user identifier and said permitted activity said user is authorized to conduct.

46. The computer program product of Claim 40, wherein said 5 computer readable program code additionally causes said programmable computer processor to provide in said user table a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct.

10 47. The computer program product of Claim 40, wherein said computer readable program code additionally causes said programmable computer processor:

to provide a class table comprising at least a unique class identifier for each authorized class of users and at least one 15 permitted activity said class of users is authorized to conduct with respect to said data storage media, said class identifier, when combined with a user authentication message from a user of said authorized class of users in accordance with said predetermined algorithm, authorizes said user;

20 in conducting said combination, upon receiving said user authentication messages from said data storage drive via said wireless interface, to combine said user authentication message

DOCKET: TU999050

with said class identifier from said class table in accordance with said predetermined algorithm to authorize or deny said class activity to said user; and

in conducting said transmission, to transmit said class 5 authorization or denial to said data storage drive via said wireless interface.

48. The computer program product of Claim 47, wherein said computer readable program code additionally causes said programmable computer processor to provide in said user table any 10 class membership of each said user, wherein said user may be authorized with respect to said class table either by said class authorization or by said user authorization.

49. The computer program product of Claim 47, wherein said computer readable program code additionally causes said 15 programmable computer processor to provide in said user table and said class table a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising 1) read access to data stored in said data storage media, 2) write access to data stored 20 in said data storage media, 3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table.

DOCKET: TU999050

50. The computer program product of Claim 40, wherein said data stored in said data storage media is encrypted, and wherein said computer readable program code additionally causes said programmable computer processor to provide in said user table 5 permitted activities comprising at least 1) read access to data stored in said data storage media, and wherein said computer readable program code additionally causes said programmable computer processor to transmit in said user authorization for said read access, a decryption key for said encrypted stored data.

**WIRELESS SECURITY ACCESS MANAGEMENT
FOR A PORTABLE DATA STORAGE CARTRIDGE**

ABSTRACT

A portable security system mounted in a portable data storage cartridge for managing access by users to the cartridge. A programmable computer processor mounted in the cartridge is powered by and receives data from and transmits data to a data storage drive via a wireless RF interface, when mounted in the drive. A user table has a unique user identifier for each authorized user and lists permitted activities the user is authorized to conduct with respect to the data storage cartridge. Preferably, a private key, public key algorithm is employed. Thus, the user identifier comprises a user symbol and a user decrypting sender public key. A user authentication message from the authorized user is encrypted by a sender private key and a receiver public key, in accordance with a predetermined algorithm, employing the cryptographic algorithm. The cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key, whereby the user authentication message is known to have come from the user. Then, the security system algorithm grants access to the user for the listed activities with respect to the cartridge.

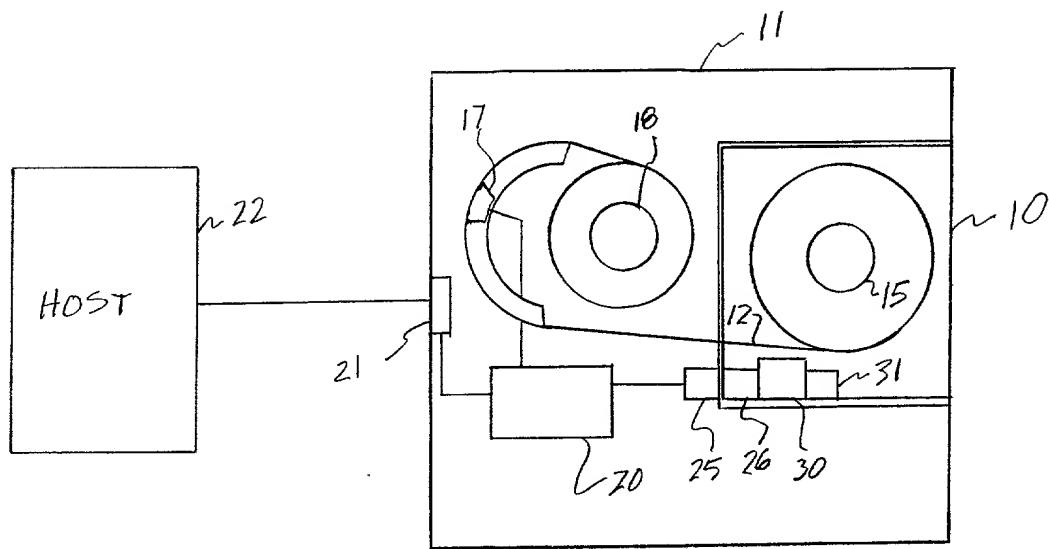


FIG. 1

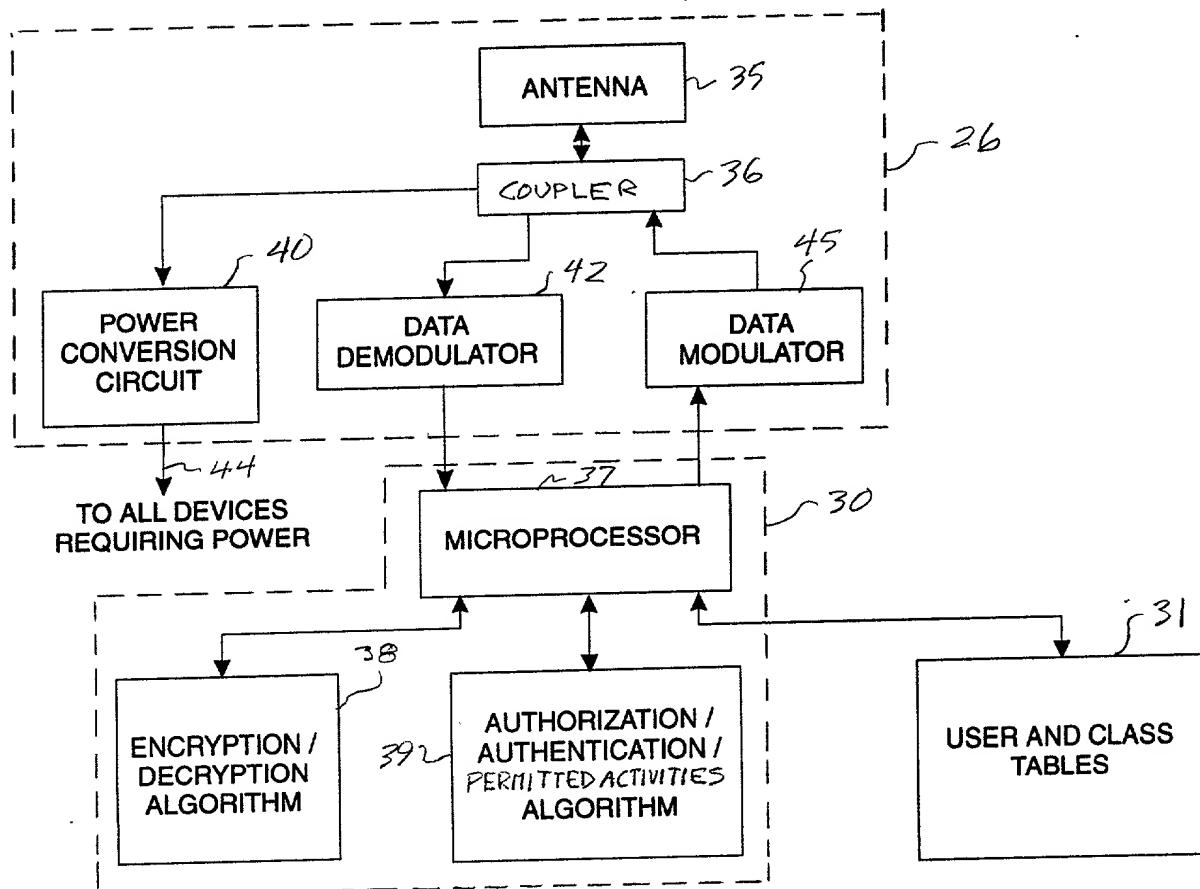


FIG. 2

UNINITIALIZED CARTRIDGE

10
↳

User Table: empty
Class Table: empty

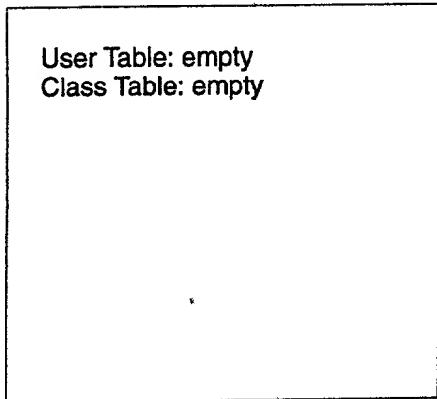
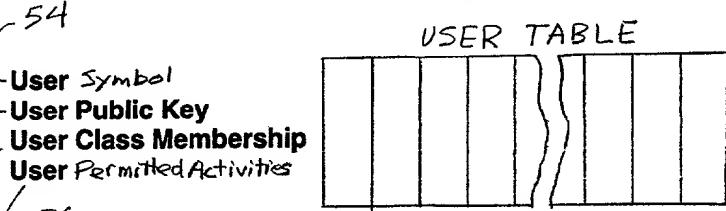


FIG. 3

INITIALIZED CARTRIDGE

10
↳



62 Class Symbol
Class Public Key
Class Permitted Activities

63
64

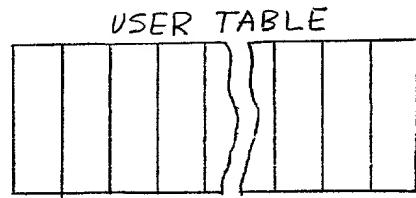


FIG. 4

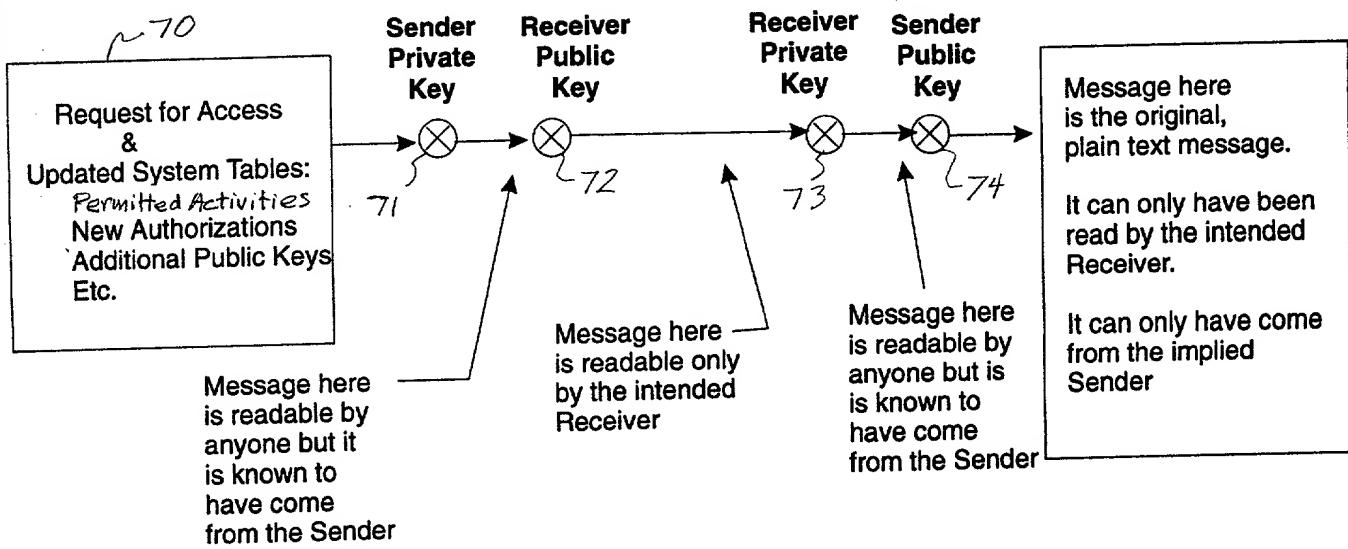


FIG. 5

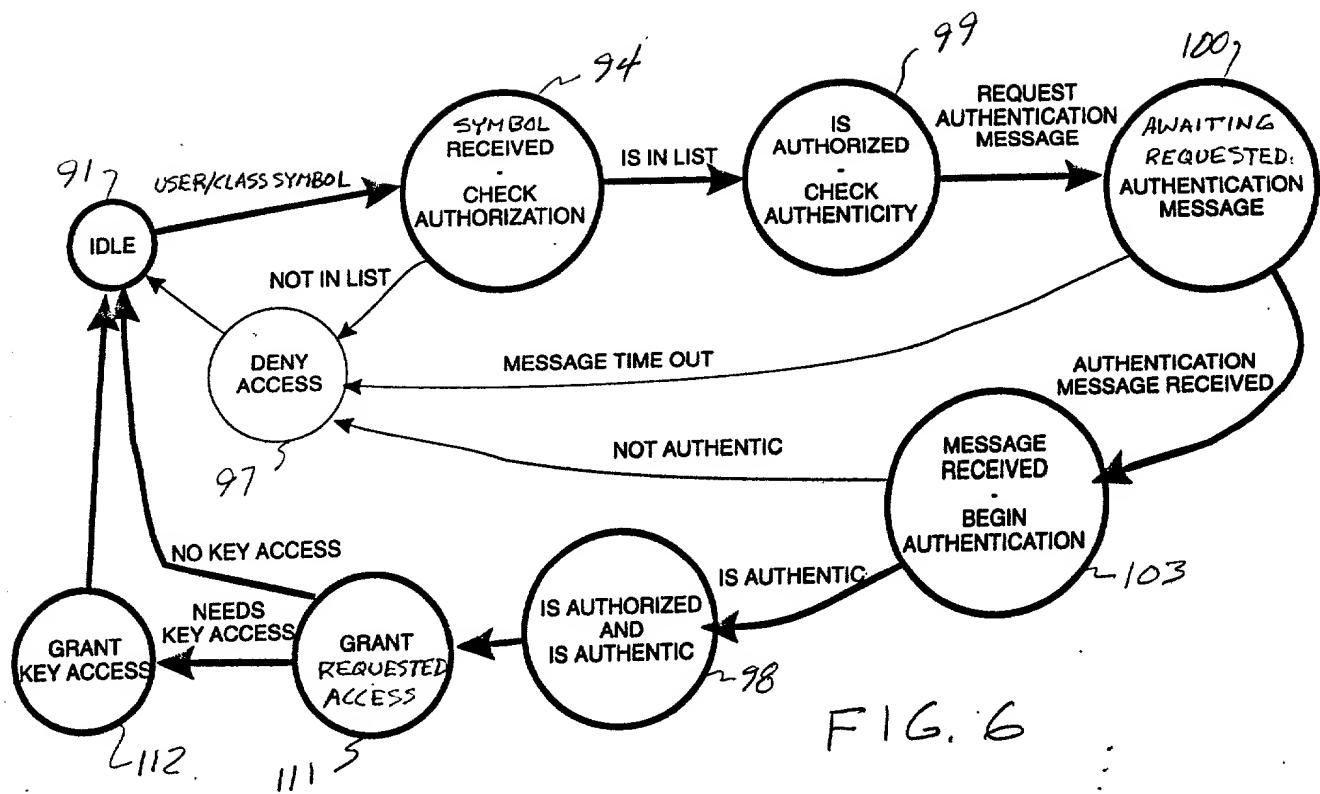


FIG. 6

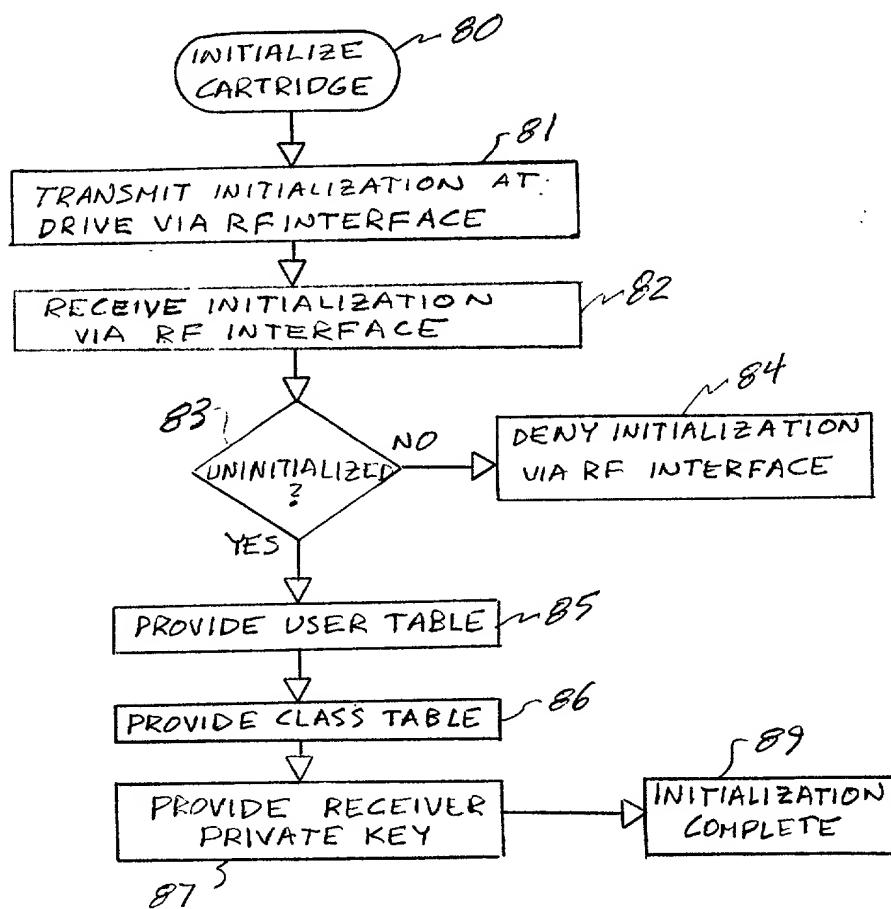


FIG. 7

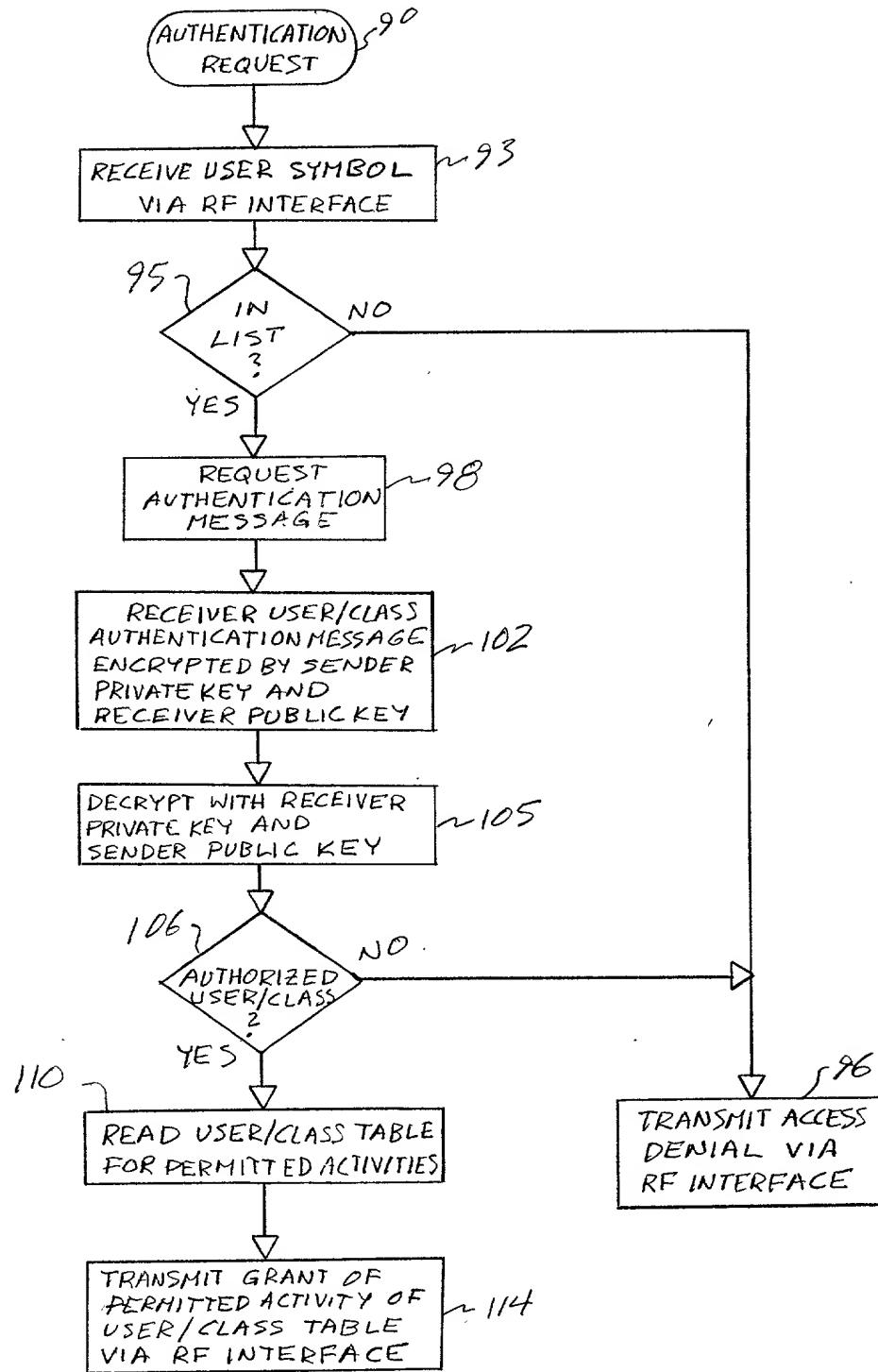


FIG. 8

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

WIRELESS SECURITY ACCESS MANAGEMENT FOR A PORTABLE DATA STORAGE CARTRIDGE

the specification of which (check one)

is attached hereto.

was filed on _____

as Application Serial No. _____

and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)	Priority Claimed
<input type="checkbox"/> None <input type="checkbox"/> (Number) _____	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> (Country) _____ (Day/Month/Year Filed) _____

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56, which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

<input type="checkbox"/> None <input type="checkbox"/> (Application Serial No.) _____	<input type="checkbox"/> (Filing Date) _____	<input type="checkbox"/> (Status) (patented, pending, abandoned)
--	--	--

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

John H. Holcombe (#20,620)
Philip R. Wadsworth (#29,219)
John E. Hoel (#26,279)
G. Marlin Knight (#33,409)
Monica D. Lee (#40,696)
Robert B. Martin (#26,945)
Joseph C. Redmond (#18,753)
Joseph F. Villella, Jr., (#30,599)

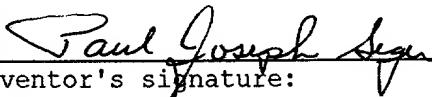
Robert M. Sullivan (#39,391)
Christopher A. Hughes (#26,914)
Esther E. Klein (#34,337)
Noreen A. Krall (#39,734)
Douglas R. Millett (#31,784)
Edward A. Pennington (#32,588)
Paik Saber (#37,494)

Send correspondence to:

Robert M. Sullivan
IBM Corporation
Intellectual Property Law
9000 S. Rita Road (90A/9032)
Tucson, Arizona 85744

Direct Telephone Calls to: (name and telephone number) John H. Holcombe, 520-760-6629

Full name of sole or first joint-inventor: PAUL JOSEPH SEGER


Inventor's signature:

November 3, 1999
Date:

Residence: 5145 W. Paseo Del Barranco, Tucson, Arizona 85745

Citizenship: USA

Post Office Address: Same